

EXHIBIT B



December 20, 2023



40 2 13593 *****AUTO**ALL FOR AADC 125

IAN W WERKMEISTER



Dear Ian W Werkmeister,

I am writing to inform you of an incident that may have involved your personal information. On October 19, 2023, Wayne Bank was notified by a third-party Information Technology (IT) service provider of a data security incident that involved unauthorized access to a number of its financial institution clients' customer data, including Wayne Bank customer information, in one of their file transfer applications, MOVEit. Please note, the vulnerability discovered in MOVEit **did not** involve any of Wayne Bank's internal systems and **did not** impact our ability to service our customers.

The incident involved vulnerabilities discovered in MOVEit Transfer, a file transfer software used by our vendor to support services it provides to Wayne Bank and its related institutions. MOVEit is a commonly used secure Managed File Transfer (MFT) software, which supports file transfer activities used by thousands of organizations around the world, including government agencies and major financial firms.

Our service provider launched an investigation into the nature and scope of the MOVEit vulnerability's impact on its systems and discovered that the unauthorized activity in the MOVEit Transfer environment occurred between May 27 and 31, 2023, which was before the existence of this vulnerability was publicly disclosed. During that time, unauthorized actors obtained our vendor files transferred by MOVEit. These files included Wayne Bank and related institution customer information, including yours.

From a careful review of the contents of the files, we have determined that one or more of the files may have contained information including your name, Social Security number (full number), date of birth, account number (full), and routing number / ABA number.

Wayne Bank takes the protection of your personal information very seriously and, upon learning of this incident, immediately launched a comprehensive investigation. Our service provider advises us that they have remediated the technical vulnerabilities and patched the systems in accordance with the MOVEit software provider's guidelines. To help prevent something like this from happening again, our service provider also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities. We will contact you if we learn anything further that would be pertinent to your account.

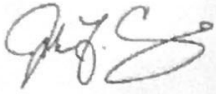
In order to help assure you that your personal information is protected, **we have arranged for you to receive complimentary free identity monitoring service through Kroll for two years.** Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

For more information on identity theft protection, including instructions on how to activate your free identity monitoring, as well as some additional steps you can take for your protection, please review the documents enclosed with this letter.

Regardless of whether you elect to activate the identity monitoring service, we strongly recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your bank account statements and notify us or any of your other financial institutions if you suspect unauthorized activity.

Please be assured that we are taking steps to address this incident and help protect the security of your personal data. A special customer call center has been set up to answer any questions you may have about the incident. Please feel free to contact the center at 866-799-0690, Monday-Friday, 9:00 a.m. to 5:00 p.m. Eastern Time, during standard business days.

Sincerely,

A handwritten signature in dark ink, appearing to read "John Carmody". The signature is stylized with a large, sweeping "C" and a long, horizontal stroke at the end.

John Carmody
Executive Vice President and
Chief Credit Officer
Wayne Bank

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **March 26, 2024** to activate your identity monitoring services.

Membership Number: E3NH65638-P

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

PROTECTING AGAINST IDENTITY THEFT AND FRAUD

Place a Fraud Alert on Your Credit: To protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit agency files.

A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days.

To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each.

- Equifax (888) 766-008 or www.fraudalert.equifax.com
- Experian (888) 397-3742 or www.experian.com
- TransUnion (800) 680-7289 or www.transunion.com

You may also consider placing a **Security Freeze** on your credit reports. A Security Freeze prevents most potential creditors from viewing your credit reports and therefore, further restricts the opening of unauthorized accounts.

Your state Attorney General may also have advice on preventing identity theft. Contact information for these entities is listed below.

- **Federal Trade Commission:**
Visit www.ftc.gov/bcp/edu/microsites/idtheft
- **Pennsylvania Attorney General**
Call (717) 787-3391 or visit <https://www.attorneygeneral.gov/protect-yourself/identity-theft>
- **New York Attorney General**
Call (800) 771-7755 or visit <http://www.ag.ny.gov>
- **New York Department of State Division of Consumer Protection**
Call (800) 697-1220 or visit <https://dos.ny.gov/consumer-protection>
- **Florida Attorney General**
Call (866) 966-7226 or visit <https://www.myfloridalegal.com/identity-theft/identity-theft-victim-kit>
- **New Jersey Attorney General**
Call (609) 984-5828 or visit <https://www.nj.gov/njsp/tech/identity.html>